Dr. M.G.R

EDUCATIONAL AND RESEARCH INSTITUTE

DEEMED TO BE UNIVERSITY

University with Graded Autonomy Status

(An ISO 21001 : 2018 Certified Institution)
Maduravoyal, Chennai - 600 095, Tamilnadu, INDIA

IT Policy

Institution has an IT policy, makes appropriate budgetary provision and updates its IT facilities including Wi-Fi facility

Vision and Mission Statement of Dr. MGR Educational and Research Institute information Technology policy:

Vision:
- To provide Modern IT infrastructure and make all university materials and services ITenabled.

Mission:
- To upload the information technology infrastructure systematically and technology remains up to date.
- To provide confident and secure IT infrastructure that can provide a platform for all type of information, statics and dynamics. University has the following state of the art IT infrastructure

Dr MGR - IT Policy

Dr. MGR Educational and Research Institute has clear policy regarding Information Technology ,The University always leads in adopting latest technologies and providing IT enabled service to all its stakeholders. The policy provides a framework how to utilize IT infrastructure and also lays down Vision and Mission of the University in building all its job IT enabled. It also rough out a mechanism for establishing and maintaining the IT infrastructure at University main campus and all its other campus. The University has appropriate budgetary provision for expansion and updating its IT facilities including wi-Fi. These policies apply to all faculty, staff, and students of the University, Data Stewards (those that manage access to data and IT resources) and anyone who uses University IT resources.

The following IT Policies cover among other things, the following aspects:

Use of IT Resources :
Information technology (IT) resources must be utilized respectfully and as authorized and designed. While utilizing University-owned IT resources, no user or administrator is authorized to engage in any activity that violates University policy or any illegal activity under local, state, central or internationallaw.

Access Control Policy:
All University information technology (IT) resources that store, process, or transmit Confidential or Protected data must require usernames and passwords for access. Prior authorization is mandatory for access to the University's IT resources that store, process or transmit Confidential or Protected Data.

User Names and Passwords:
Data Administrators will configure systems and applications to meet the following requirements to authentic users of IT resources that store, process or transmit Confidential or Protected Data, Data Administrators must assign each user a unique login name. Login names will have an associated password, which is required to minimally meet the standards for secure password and as per University requirements. Users must not share account passwords with any otherperson.

Free and Opensource Software:
The University advocates the use of Free and Open Source Software. Where proprietary

software is required for certain essential activities of the University, as far as possible, software that are compatible with a free operating system such as Linux will beused.

Ownership of Software: All knowledge resources developed by faculty, staff, students or contract personnel on behalf of the University or licensed for the University's use is the property of University and must not be copied for use at home or any other location, unless otherwise specified by the licenseagreement.

Installed Software:

While the university advocates the use of free and opensource software, whenever proprietary software is required to be used, all such software packages that reside on computers and networks within the University must comply with applicable licensing agreements and restrictions and must comply with the University's acquisition of softwarepolicies.

Security Concern:

Approved virus checking systems must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checkingsystems.

Secure Web Application:

Departments will ensure that development, test, and production environments are separated. Confidential Data must not be used in the development or test environments. All applications must be tested for known security vulnerabilities prior to being placed in production and at regular intervalsthereafter.

Use of Official Email lists:

As part of the University's ongoing activities to improve communication and leverage its investment in technology, University IT services created Official Email Lists to help the University conduct its communication with targeted audiences. In order to ensure that faculty and staff would not be inundated with mass e-mailings, oversight procedures were put in place to monitor the email messages being sent via the official emaillists.

Network Security:

The university campuses have completely switched, high availability voice enabled network. Network has a layered architecture consisting of Security, Core, Distribution and Access layer. The users are segregated into different categories and each category can have different access . This is achieved by dividing the entire network into different logical network and access to these logical network is controlled by implementing the desired access policy.

Significant of Data : The policy outlines the roles and responsibilities of Data Stewards, Data Administrators and Data Users.

IT Security Awareness Training: University maintains an Information Security Awareness Training program that supports the University employees' and students' needs for regular training, and reminders to enable them to appropriately protect University information technologyresources.

Green Computing :

University strives hard to reduce the carbon footprint . Most of the administrative activities pertaining to faculty, staff and student are handled through the ERP servers placed in data centre. All the notices are electronically circulated through e-mails. The e-mail confirmation is allowed and is preferred over printed letters. All the news feeds are displayed through networked LCD TVs.

University strictly discourages the use of printers and printed materials. The power reduction is managed by replacing the older and power hungry technology /devices with newer devices requiring less power eg. replacement of CRT monitors with LCD monitors .

Computing facilities -Hardware infrastructure:
The university has established very good computing infrastructure. It has available over 5000+ computer systems in the laboratories of the university and administrative offices. This ensures a Computer-student ratio of 1:1.

- Computers(3500+ no's),
- Servers(10 no's),
- Data Centre
- Storage
- Projectors(10 no's),
- Printers

Networking infrastructure:

- LAN(3500 + nodes)
- Wi-Fi network50+ access points.
- Active and passive components for networking
- Core Switch – Juniper EX-4200
- Firewall Security System, internet applications – SOPHOS SX340

Internet Availability

All campus of the University is accomplished by high speed network and Wi-Fi facility with around 3500+ nodes. Airtel Fiber optic cables are available for faster and efficient connectivity. Old and outdated computers are upgraded periodically. They are either replaced or enhanced with respect to configuration. Enhanced computing facilities are added based onthe requirements of students, research scholars and faculty.

1) Bandwidth details:100 Mbps internet leased line, 10 Mbps backup line.

2) LAN Facility details
3500+ nodes LAN with OFC backbone

3) Wi FI details
Centralized controller with 50+ Access points

4) Firewall details
Unified Threat ManagementSOPHOS SX340 next generation firewall.

5) Antivirus details:
Secrete End point Security, K-7 Anti virus

6) Exchange up gradation in calling service
    Servers and desktops, Network centre are upgraded at regular interval of Time

7) Software details (academic, examination, Server, Language base software)